

Home Computer and Internet User Security

Lawrence R. Rogers

Version 1.0.4

CERT® Training and Education

Networked Systems Survivability

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213-3890

© 2005 Carnegie Mellon University

® CERT, CERT Coordination Center, and Carnegie Mellon are registered in the U.S. Patent and Trademark Office

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JAN 2005		2. REPORT TYPE		3. DATES COVERED 00-00-2005 to 00-00-2005	
4. TITLE AND SUBTITLE Home Computer and Internet User Security				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 50	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Quotes to Ponder

Homeland security begins at home.

Various on the Internet

Property has its duties as well as its rights.

Thomas Drummond (1797-1840)



Goals

Aware – *Understand the issues*

- Learn about Home Computer Security issues.

Knowledgeable – *Skills to do something*

- References contain specific technology examples and checklists.

Educated – *Foundation for the future*

- Fundamental issues are highlighted.



Home Computer Security

Guide to improving the security of your home computer

Technology independent explanation

Examples using Windows 2000

Checklists



<http://www.cert.org/homeusers/HomeComputerSecurity/>



Topics

Introduction

Things you should

- know about security
- do to your home computer – tasks
- do when using any computer – practices



Topics

Introduction

Things you should

- know about security
- do to your home computer – tasks
- do when using any computer – practices



What Problem Are We Solving?

What's yours is yours until you say otherwise!

Keep computer-based possessions yours.

Examples:

- CPU cycles
- memory
- disk space and contents
 - your files
 - software you've bought
- Internet connectivity
- not a new idea
- What locks exist?
- How are they used?



http://www.cert.org/homeusers/goalof_computersecurity.html



Crime on the Internet

Means +

- software or wetware

Motive +

- Anything worth stealing on the Internet?

Opportunity =

- Internet access readily available

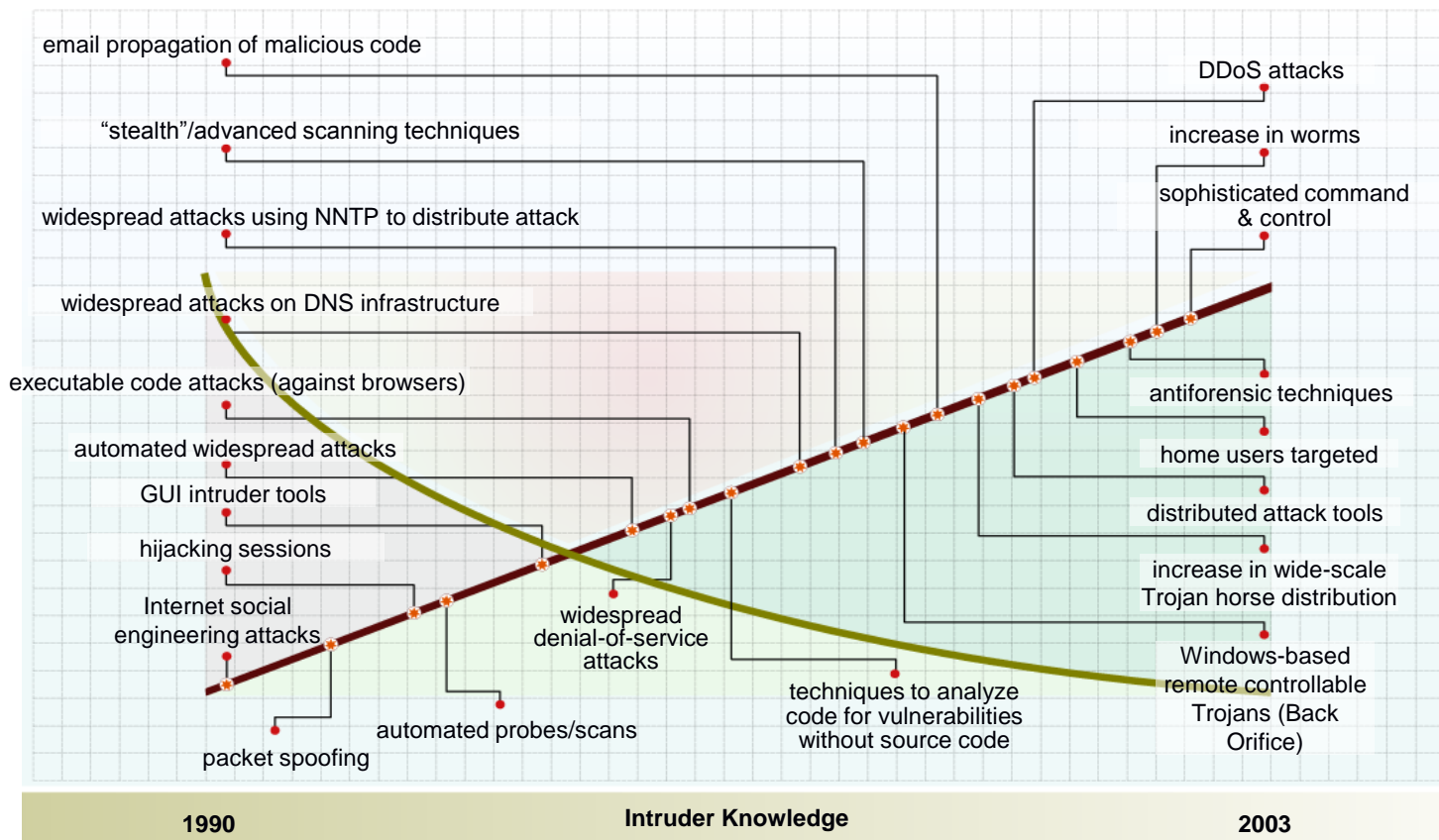
Internet crime!



<http://www.cert.org/homeusers/mmo.html>



Attack Sophistication vs. Intruder Technical Knowledge





Why Should I Care?



You are probably either

- a professional or SA at the office
- an owner of a home computer

Therefore, you are a system administrator!

- same responsibilities
- same tasks

And, for home computers

- they are a prime target
- because they are less secure

http://www.cert.org/homeusers/ira_sysadmin.html



Topics

Introduction

Things you should

- **know about security**
- do to your home computer – tasks
- do when using any computer – practices



Trust -1

We are trusting by nature.

The Internet is built on trust.

But the world has changed.

Trust by itself is no longer sufficient.

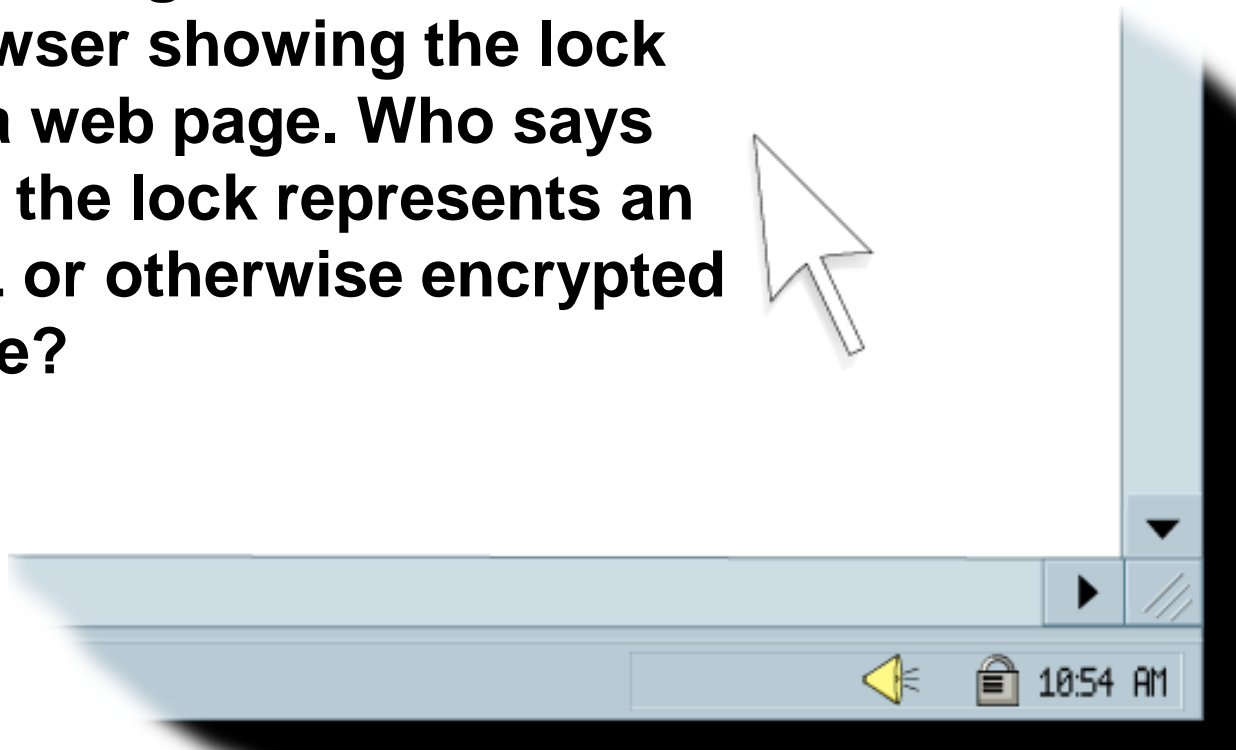
Consider a cereal box.





Trust -2

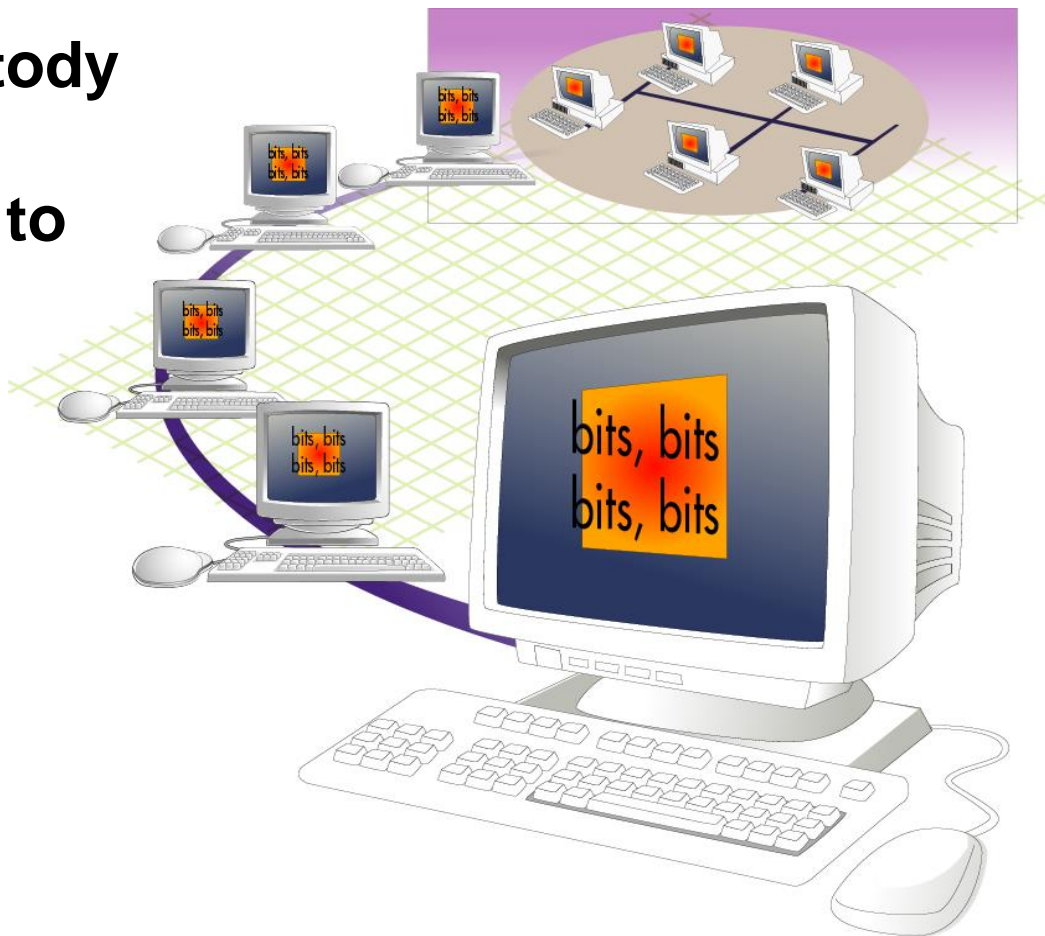
Now imagine a web browser showing the lock on a web page. Who says that the lock represents an SSL or otherwise encrypted page?





Trust -3

**Chain of custody
of bits, from
construction to
consumption**





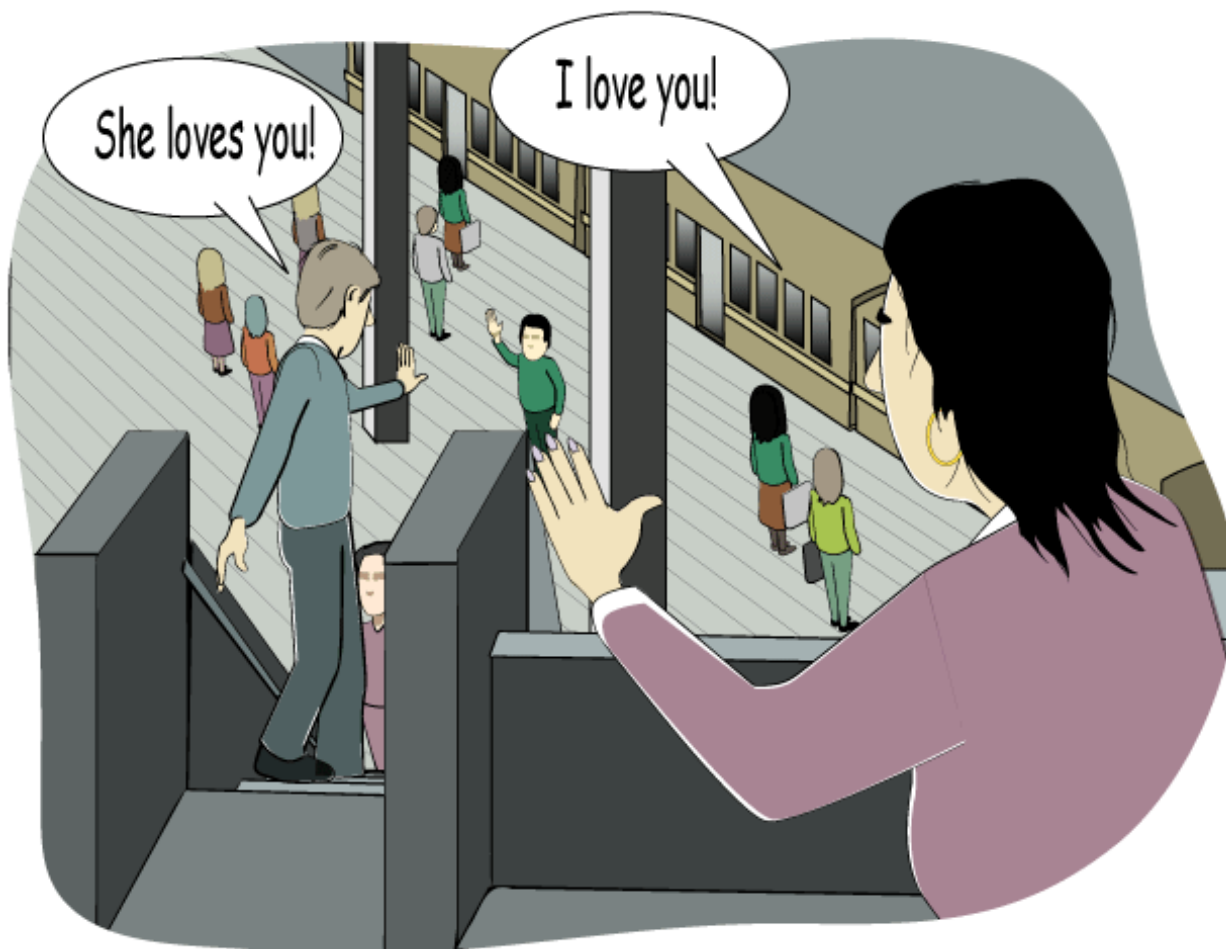
Information in the Clear



Eavesdropping
Identity theft
Dumpster diving

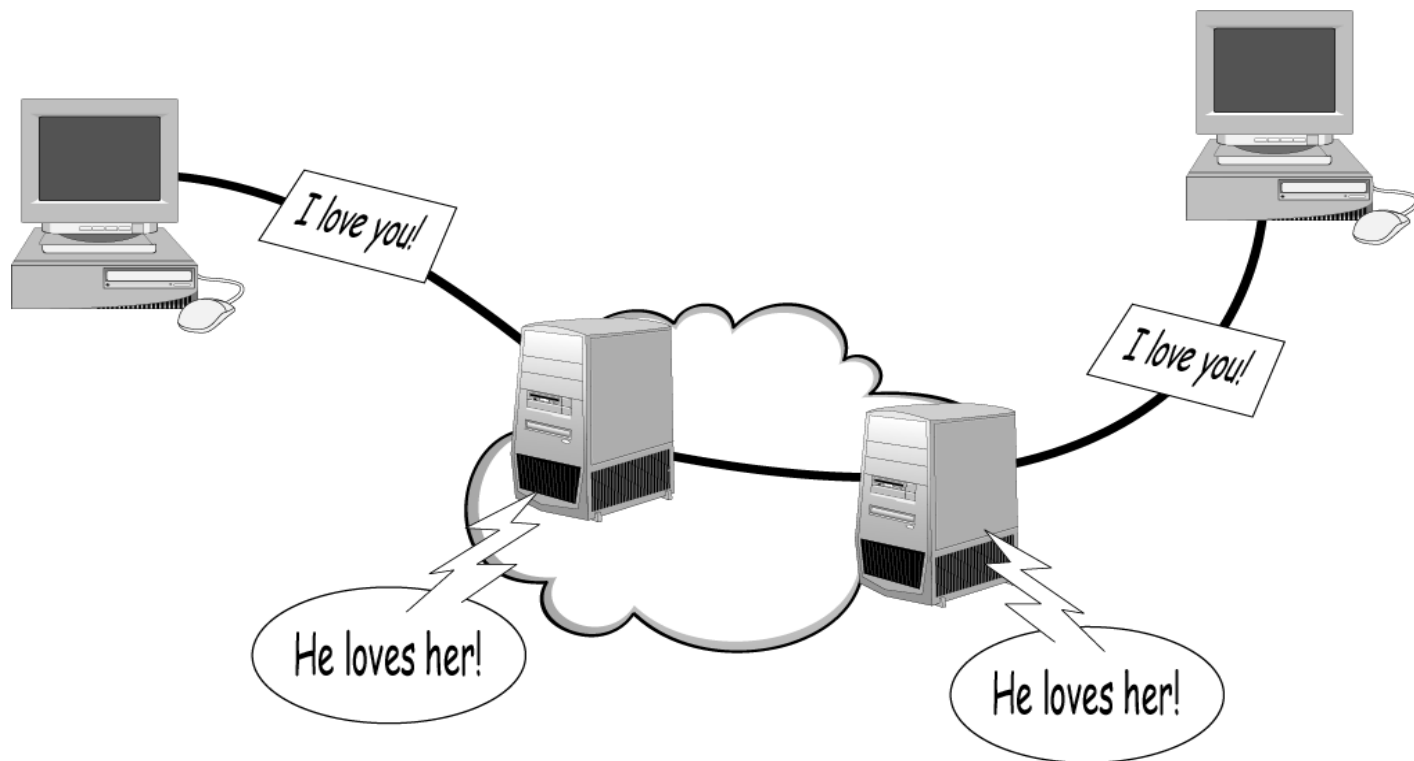


How the Internet Works -1





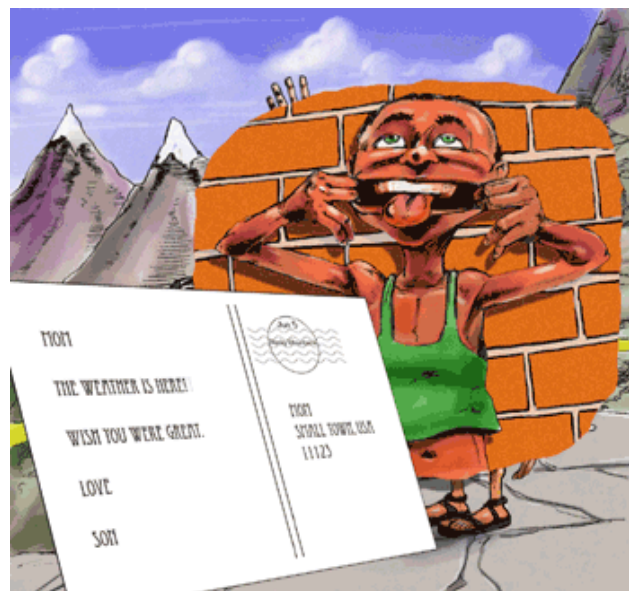
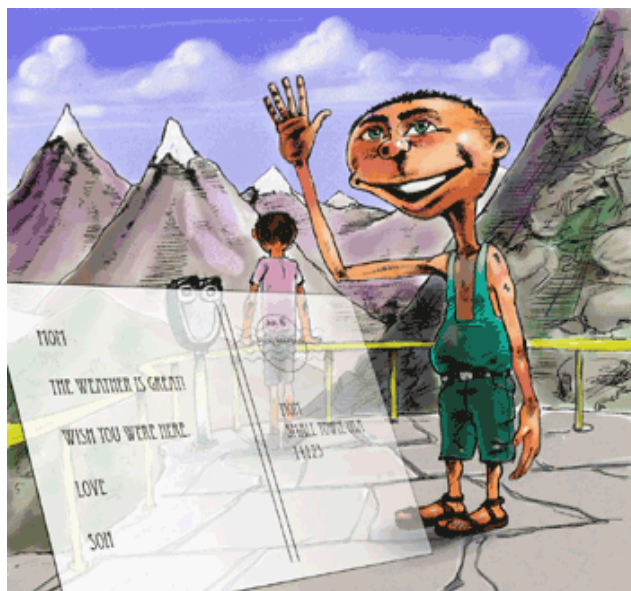
How the Internet Works -2





Email is in the Clear

Email – A Postcard Written in Pencil



http://www.cert.org/homeusers/email_postcard.html



Topics

Introduction

Things you should

- know about security
- do to your home computer – tasks
- do when using any computer – practices



The Nature of Maintenance

All things to “do” are straightforward.

When new, they may even be “fun.”

However, they can get old.

The challenge is to continue to do the task.

Levels of effort required to maintain:

- **low – setup plus light maintenance (“fire and forget”)**
- **medium – setup plus medium maintenance**
- **high – setup plus significant maintenance**



Task: Install and Use Antivirus Software

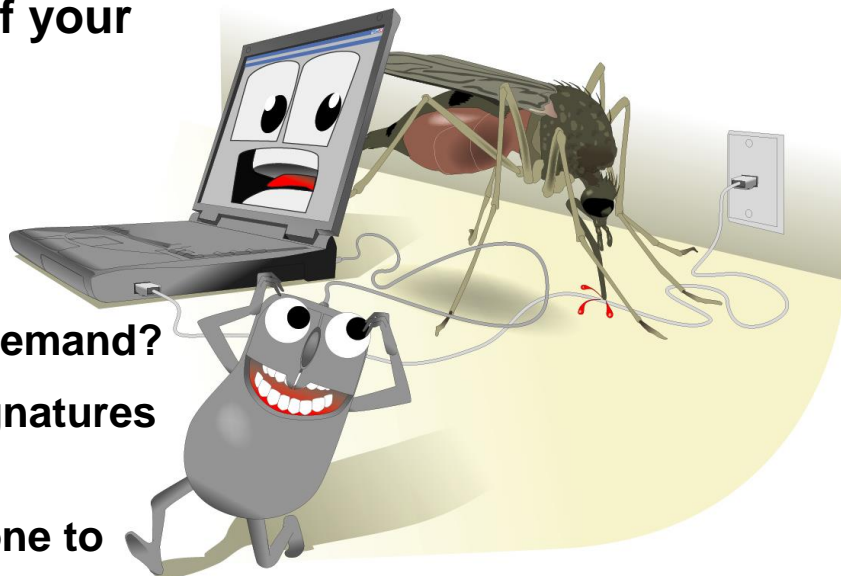
Easy way to gain control of your computer or account

Violates “trust”

DURCH tests

- Demand – Check files on demand?
- Update – Get new virus signatures automatically?
- Respond – What can be done to infected files?
- Check – Test every file for viruses.
- Heuristics – Does it look like a virus?

Level of effort: low





Task: Keep Your Systems Patched



Unpatched programs are weak spots.

Intruders exploit these to gain access.

ABU tests

- **Affected** – Is my system affected?
- **Break** – Does this patch break something else?
- **Undo** – Can I undo patch installation?

Level of effort:

- **patching: low**
- **what breaks: medium to high**
- **undoing install: medium to high**



Task: Install and Use a Firewall Program

Limit connections to computer

Limit connections from computer based on application

Portable – follows the computer (laptop)

PLAT tests

- **Program** – What program wants to connect?
- **Location** – Where does it want to connect?
- **Allowed** – Yes or no?
- **Temporary** – Permanent or temporary?

Level of effort:

- **install: low**
- **maintain: high**





Speaking of Firewalls ...



<http://www.cert.org/homeusers/HomeComputerSecurity/#4>



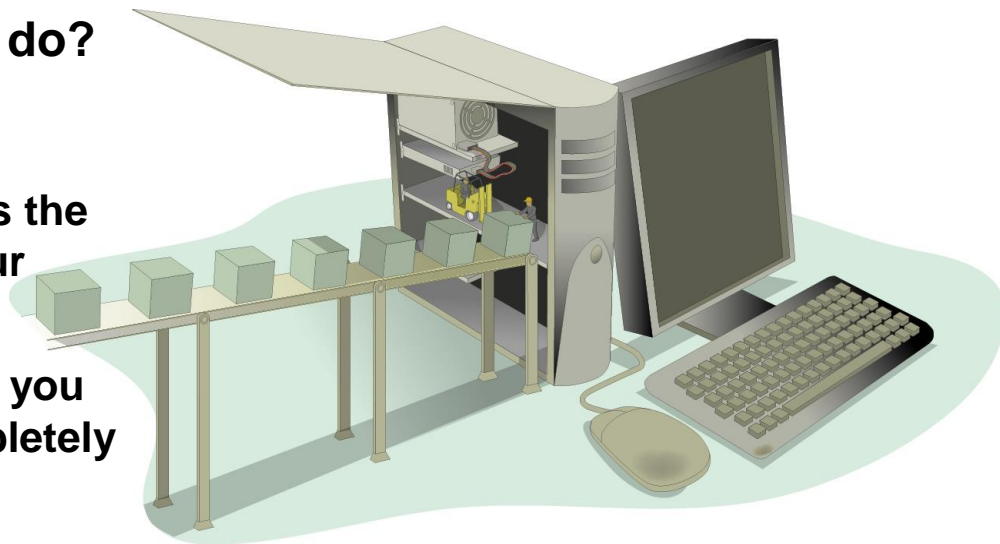
Task: Use Care when Downloading and Installing Programs

Program may satisfy needs but may harm computer

What does it *really* do?

LUB tests

- **Learn** – What does the program do to your computer?
- **Understand** – Can you return it and completely remove it?
- **Buy** – Purchase/download from reputable source?



Level of effort: high



Task: Install and Use a Hardware Firewall

Guards all computer systems at home

First layer of defense

Fast

Provides logging

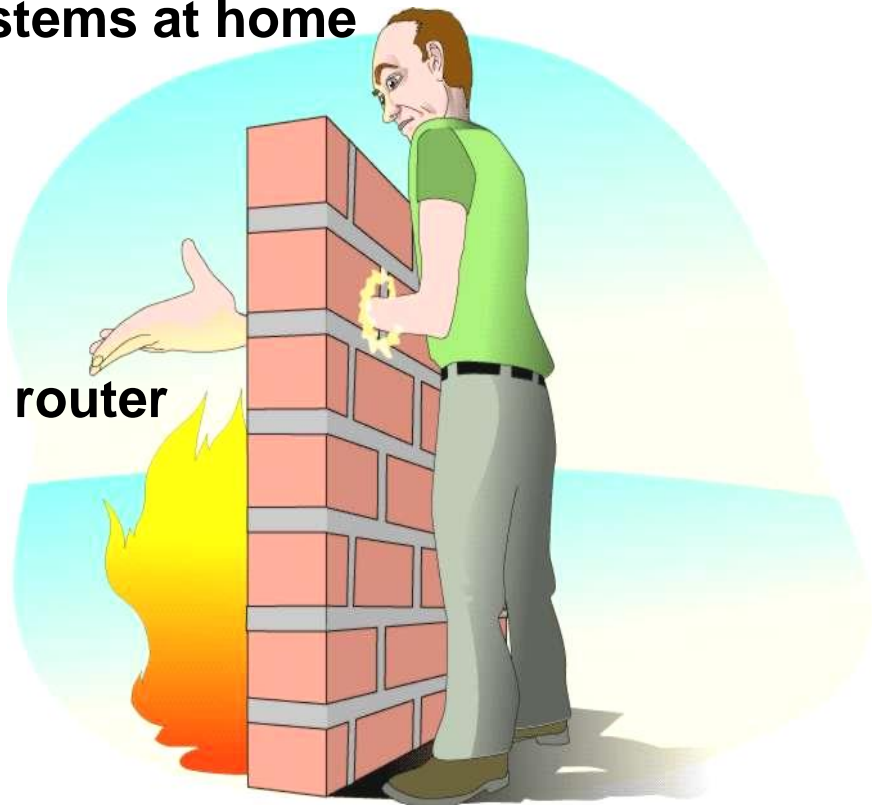
Bundled with cable/DSL router

Bundled with wireless

Default deny setting

Level of effort:

- **install: low**
- **maintain: low**



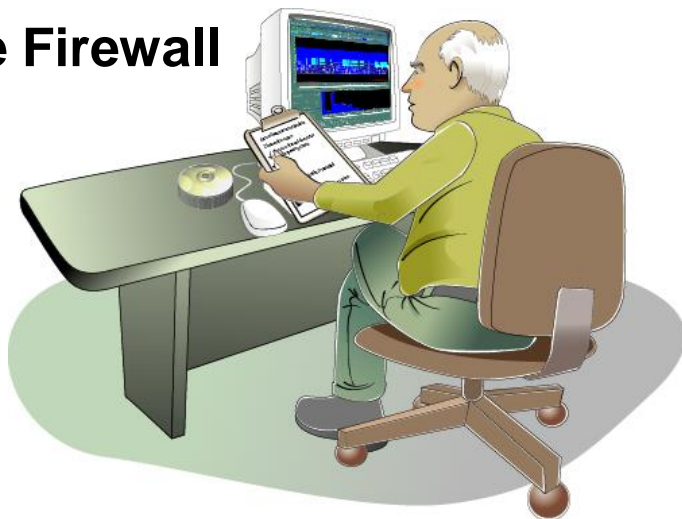


Tasks Summary

- ☐ **Install and Use Antivirus Software**
- ☐ **Keep Your Systems Patched**
- ☐ **Install and Use a Firewall Program**
- ☐ **Use Care when Downloading and Installing Programs**
- ☐ **Install and Use a Hardware Firewall**

Some easy, some not so easy

All important





Topics

Introduction

Things you should

- know about security
- do to your home computer – tasks
- **do when using any computer – practices**



What are Practices?

Practices are steps to follow no matter what computer system you are using.

A home computer is but one instance.



Practice: Use Care When Reading Email with Attachments

Executable content

Interesting to you (social engineering)

Violates trust

KRESV tests

- **Know test – Know the sender?**
- **Received test – Received email before?**
- **Expect test – Did you expect this email?**
- **Sense test – Does this email make sense?**
- **Virus test – Contain a virus?**

Doesn't pass all tests? Don't open!

Level of effort: high





Using KRESV Tests

1. **Send introductory email (Know)**
 - ask permission to send attachment
2. **Qualifies as Received**
3. **If OK, they will then Expect the email**
4. **Subject line needs to make Sense**
5. **Scan attachments for Viruses**
6. **Send the mail**

Level of effort: medium to high



Practice: Make Backups of Important Files and Folders

Can you recover a file or folder if lost?

Does your computer have a “spare tire”?

FOMS tests

- **Files** – What files should be backed up?
- **Often** – How often should a backup be made?
- **Media** – What kind of media should be used?
- **Sore** – Where should that media be stored?

Level of effort:

- **setup:** medium to high
- **maintaining:** medium





Practice: Use Strong Passwords

Passwords are like house keys

Different key for each lock

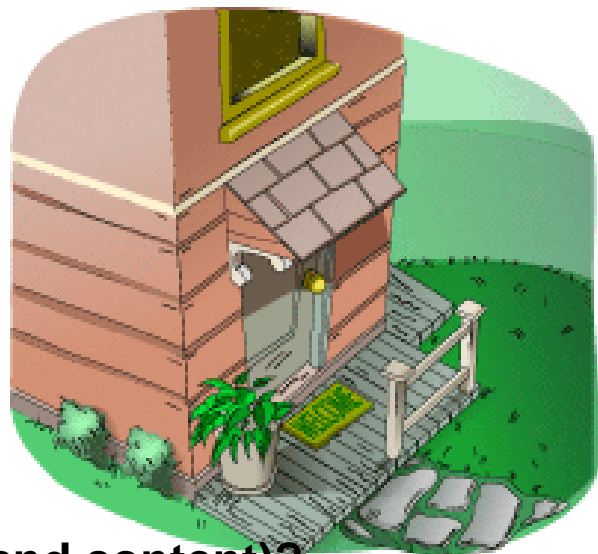
Brute force attacks

Sniffing clear text

SUPR tests

- **Strong** – Password strong (length and content)?
- **Unique** – Unique and unrelated to other passwords?
- **Practical** – Can you remember it?
- **Recent** – Have you changed it recently?

Level of effort: medium

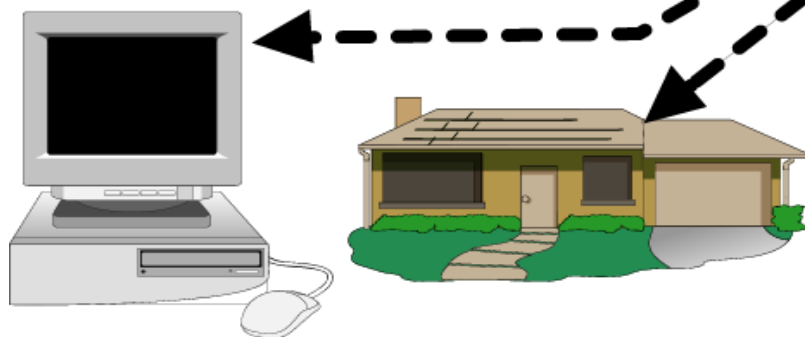




The Best Protection

Something you know
+ Something you have
+ Something you are

= The Best Protection





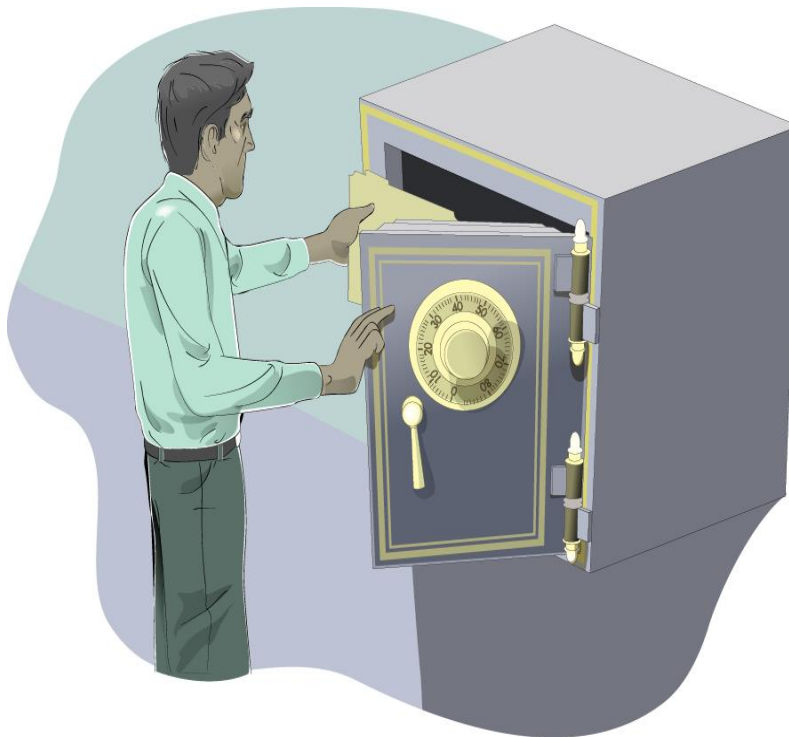
Something You Know

Username

Password

PIN

Passphrase





Something You Have

Smart cards

- multi-function

Examples

- national ID card
- driver's license





Something You Are

Face

Signature

Fingerprint

Retina

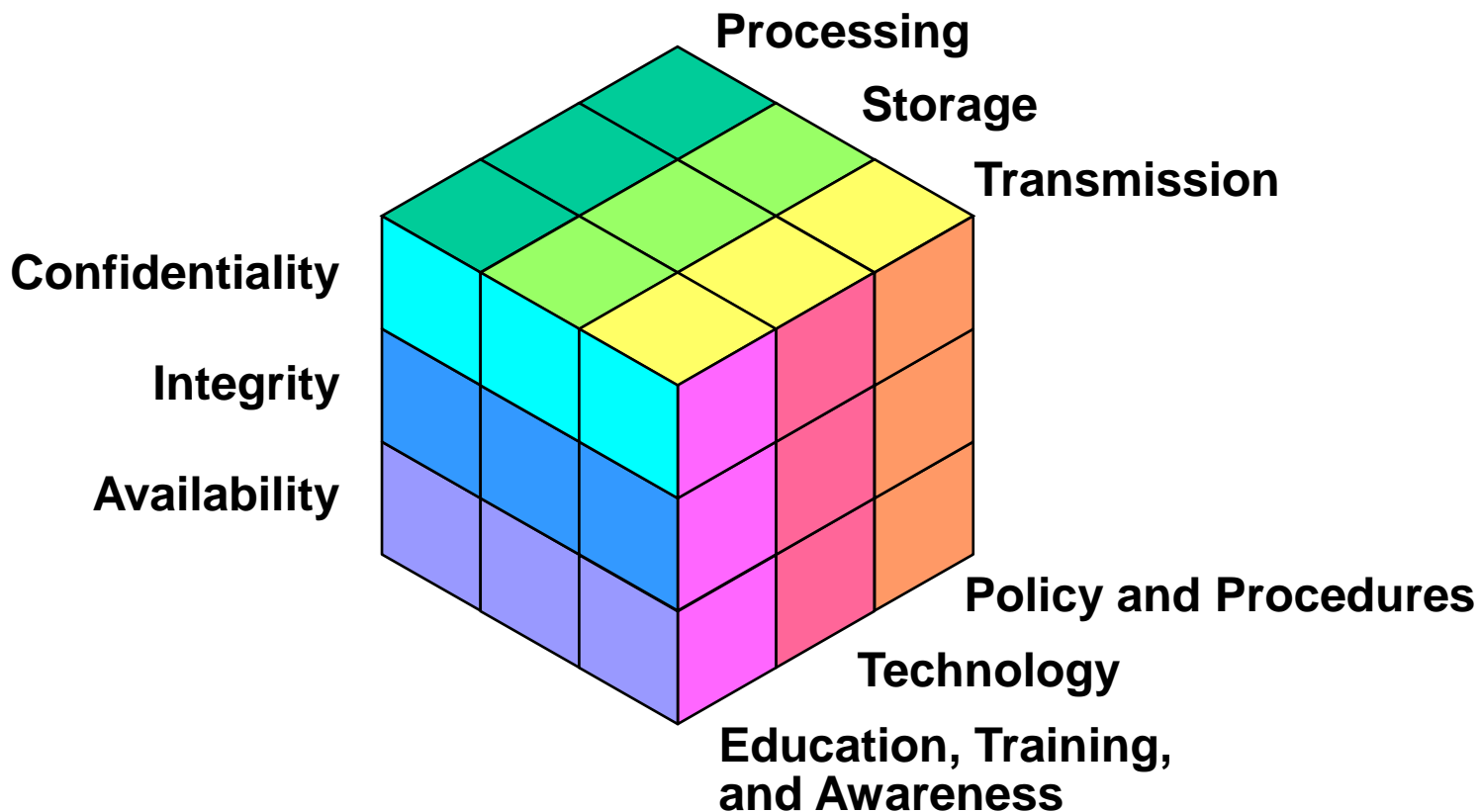
Iris

Palm geometry



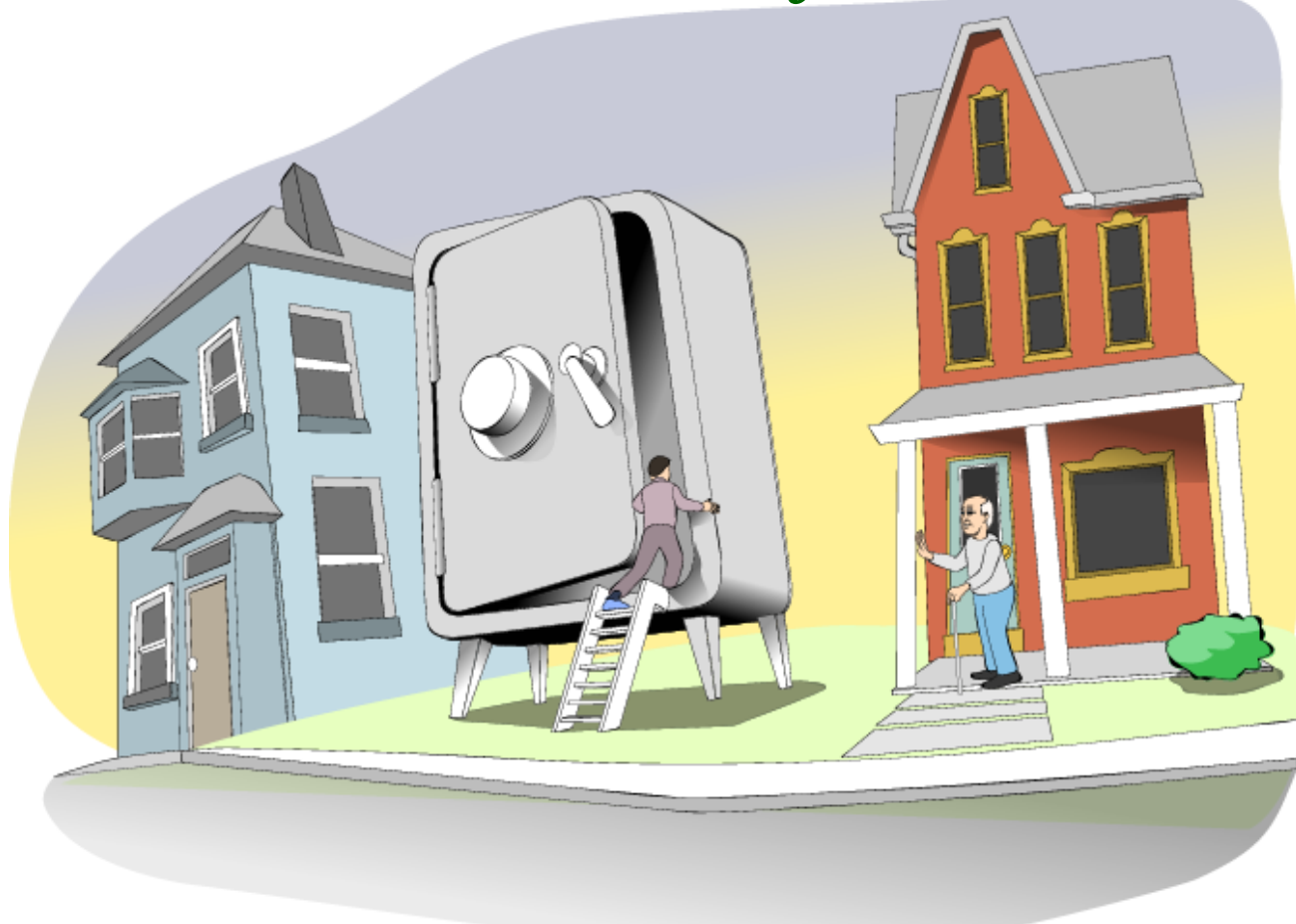


Information Security Model





Data Confidentiality – Access



<http://www.cert.org/homeusers/piglatin.html>



Internet – Friend or Foe?

Example

- SA posts question to Internet
- Gives details of network
 - hardware
 - software
 - applications
- Email address and telephone for “quick” response

What does a potential intruder now know?



http://www.cert.org/homeusers/internet_friendorfoe.html



Data Confidentiality – Encryption





Practice: Install and Use Access Controls and File Encryption

Confidentiality – Need to know only

Limit access to files and folders to only those authorized

Confidentiality of printed information

WAF tests

- Who – Which users can access?
- Access – What kind of access?
- Files/Folders – Which need access?

Level of effort: medium to high





Integrity – Can You Prove It?

Ever get a CD in the mail, at home or in the office?

How do you know where it came from?

How do you know what it contains?

What should you do with it?



<http://www.cert.org/homeusers/prove-it.html>



Practices Summary

- ☐ **Use Care When Reading Email with Attachments**
- ☐ **Make Backups of Important Files and Folders**
- ☐ **Use Strong Passwords**
- ☐ **Install and Use Access Controls and File Encryption**

Things you do everywhere

Some easy, some not so easy

All important





Knowledge – Apply to Wireless

Confidentiality

- Cannot limit access to airwaves.
- This means encryption (WEP).
- But WEP is weak.
- So use VPN or WAP.
- Disable SSID broadcasts.

Access control

- Use MAC address filtering.
- But MAC addresses can be spoofed.
- So use 802.11X for user identification.





Is There an Intruder in My Computer?

Normal

- What's normal behavior?
 - running programs
 - network traffic
 - performance
 - operating system
- hard to do
- vendors don't help

Abnormal

- need to know what normal is first

Level of effort: high



http://www.cert.org/homeusers/intruder_in_computer.html



There IS an Intruder in My Computer – What Now?

Questions to answer:

1. What changed?
 - What was there before?
 - How did it look?
2. How did they get in?
 - specific files changed
3. Why did they get in?
 - missing patches
 - out-of-date virus list
 - no firewall

Level of effort: high



<http://www.cert.org/homeusers/intruder2.html>



Questions?





References

The “Larry” Stories

(<http://www.cert.org/homeusers>)

Home Computer Security Guide

(<http://www.cert.org/homeusers/HomeComputerSecurity>)

Before You Connect a New Computer to the Internet

(http://www.cert.org/tech_tips/before_you_plug_in.html)



Contact Information

Lawrence R. Rogers

- Email: cert [@cert.org](mailto:cert@cert.org)

CERT website: <http://www.cert.org/>